DENTONS

IT Policy

Removable Media Policy

Contents

1 Purpose

The purpose of this policy is to restrict the use of Removable Media devices to access and transfer Firm data and to define standards, procedures and restrictions for Systems' Users who have legitimate business requirements for obtaining an exception to allow for the limited use of Removable Media devices to access Firm data.

2 Summary

As a general matter, the use of Removable Media devices to access or transfer Firm data is prohibited. Improper handling of removable media could result in either data loss if accessed by unauthorized parties or Firm assets being infected with malware. This policy outlines the baseline behaviors required for Systems' Users accessing Firm data via Removable Media devices to do so in a safe, secure manner.

3 Scope

This policy applies to all Systems' Users regarding the limitations of and exceptions to use Removable Media. Systems Users have a responsibility to protect the confidentiality, integrity, and availability of Firm data collected, processed, transmitted or stored on removable media. This policy supports the objectives of the overarching *Data Handling.Standard*.

4 Policy

The Firm restricts the transfer of data between Firm systems and Removable Media. Removable Media should be used only in cases where a suitable alternative is not available (e.g., Accellion, Dentons Direct).

Requests for approval or guidance should be directed to the IT department. Those granted approval should follow the exception criteria outlined below.

5 Definitions

Removable Media - storage device which can be connected to, inserted in and/or removed from a computer. Examples include optical media (e.g. CDs, DVDs), diskettes, USB flash drives, external hard drives, and memory cards (SD, Memory Stick, Compact Flash, etc.).

Systems Users - Firm’s employees, contractors, consultants, vendors, agents and those affiliated with third-parties who access the Firm’s Systems.

See *Data Classification Policy* for further detail regarding types of data.

6 Violations and Enforcement

Any person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Non-compliance with or breach of this policy will be reported to the violator’s immediate manager and/or appropriate Firm management.

7 Exceptions

Exceptions to the policy set forth above must be requested via email to the IT Security Team and/or the Office of the General Counsel or equivalent regional risk management leadership. Requests must include:

- Clear business justification for the exception
- Duration of exception request
- Any appropriate details regarding compensating controls or information that reduces the risk of the exception.

Exceptions, approved or denied, will be logged in our IT ticket tracking system for follow up and/or control purposes as appropriate.

All exceptions granted in accordance with this policy are subject to the following:

- Removable Media containing Internal, Confidential or Restricted and Highly Confidential (RHC) data must utilize full disk encryption or an encrypted file container. Encryption methods must comply with the Firm's *Encryption Policy*.
- Removable Media must be obtained from/approved by the IT Department.
- If the data is Confidential or RHC, additional file-level password protection should be used as an added layer of security.
- The recipient of the Removable Media shall be responsible for safeguarding the drive and its contents.
- If Removable Media is required and approved by a client, it is recommended that Confidential or RHC files stored on the drive be logged in our Document Management System with client/matter number for purposes of tracking, inventory and communication, and can be available in the event of a loss of the drive.
- In the event that Removable Media is lost or stolen, the Service Desk should be notified immediately, including as much detail as possible as to the data contained on the drive. This will be escalated to Information Security and/or Office of General Counsel or equivalent regional risk management leadership as appropriate.
- When the Removable Media is no longer required, the Service Desk should be notified for proper handling.
- For Removable Media usage that occurs on an on-going basis, additional policies and procedures may apply.

Appendix 1: Document control

Ownership and responsibility

Document Owner	IT Security Team
Author	Michele Gossmeyer / Andrey Zelenskiy / Travis Haag
Contact for amendments	IT Security Team

Amendment History

Date Issued	Issued by	Reason for Change
23-July-2018	IT Security Team	Annual review and updates to language to expand and refine definitions of types of media and to align data terminology with other updated policies. Distribution held for further review with OGC on terminology and exceptions.
6-May-2019	IT Security Team	Updated to reflect removable media usage restrictions
21-Aug-2020	IT Security Team	Annual review and minor revisions to remove data type definitions

Distribution List

This document has been issued to the following people for information (I) and / or review (R):

Name	Position	I / R
Eddie Reich	US General Counsel	R
Karl Hopkins	Global Chief Security Officer	I

Related Documentation

Reference	Doc Reference
Encryption Policy	106406599
Data Classification Policy	83519541
Data Handling Standard	83519566

Approval

Name	Role	Date	Comments
Michele Gossmeyer	Director, Information Governance & Compliance	20-July-2016	
Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	5-May-2019	In conjunction with OGC
Michele Gossmeyer	Global Director, Information Governance, Risk & Compliance	21-Aug-2020	